

6. The Commission has asked for comments on the application of the statutory criteria of Section 107(b) to the development of an appropriate technical standard for delivery of conference call content. Notice ¶ 79. As an initial matter, we reiterate here a more general point made above: the criteria of Section 107(b) are directed at determining how identified deficiencies in industry standards are to be cured, not whether they are to be cured. Thus, if the Commission adheres to its tentative conclusion that carriers must provide law enforcement with the content of communications on all legs of conference calls in order to meet the assistance capability requirements of Section 103, then the J-Standard must be revised to include that capability. The criteria of Section 107(b) are relevant only to how that revision is carried out.

Section 107(b)(1) calls for technical standards that "meet the assistance capability requirements" of Section 103 "by cost-effective methods." 47 U.S.C. § 1006(b)(1). In calling on carriers to provide access to all legs of conference calls, the government is not seeking to dictate the technical details of implementation decisions. Cf. 47 U.S.C. § 1002(b)(1)(A) (CALEA does not authorize law enforcement agencies to "require any specific design of equipment, facilities, services, features, or system configurations to be adopted"). As a result, manufacturers and carriers are free to employ whatever software and/or hardware modifications will provide the required call content in the most cost-effective manner. We should add that if a carrier does not provide a conference calling service that permits other parties to speak with each other when the subject has placed them on hold or has dropped off the call, nothing in the government's proposal requires the carrier to incur the cost of adding such a feature; the government seeks only to ensure that if a carrier chooses to provide its subscribers with this kind of conference calling service, law enforcement is provided with access (pursuant to legal authorization) to the communications taking place through that service.

Section 107(b)(2) calls on the Commission to "protect the privacy and security of communications not authorized to be intercepted." 47 U.S.C. § 1006(b)(2). Requiring carriers to provide law enforcement with the content of "held" legs of conference calls is consistent with this goal because law enforcement, acting pursuant to an appropriate Title III order, is authorized to acquire this call content. As explained in our prior filings, Title III does not restrict law enforcement to intercepting communications in which the subscriber or intercept subject participates, but rather encompasses all communications taking place over the facilities under surveillance. See Government June Reply Comments at 22-30. To the extent that conversations on "held" legs of conference calls may happen to involve matters unrelated to criminal activity, law enforcement's statutory obligation under Title III to "minimize" the interception of such conversations (see 18 U.S.C. § 2518(5)) provides the requisite protection for privacy interests.

Section 107(b)(3) calls for the Commission to "minimize the cost of * * * compliance on residential ratepayers" when correcting deficiencies in industry technical standards. 47 U.S.C. § 1006(b)(3). In the absence of specific cost information from carriers or manufacturers, it is difficult to evaluate what effect the full implementation of Section 103(a)(1) with respect to conference call content will have on residential ratepayer costs, but the government does not anticipate that the impact will be significant. As noted above, the language of Section 107(b)(3) presupposes that the Commission must require "compliance" with Section 103; the only question is whether the cost of compliance on residential ratepayers can be minimized in some fashion. Leaving manufacturers and carriers free to select the most cost-effective means of implementing this capability should tend to minimize any financial impact on residential ratepayers.

Section 107(b)(4) directs the Commission to establish technical standards that "serve the policy of the United States to encourage the provision of new technologies and services to the public." 47 U.S.C. § 1006(b)(4). There is no reason to expect that any technical standard regarding conference call content that may be adopted pursuant to this proceeding, whether framed by the Commission itself or by TR45.2 (see pp. 30-32 supra), will interfere with a carrier's ability to provide "new technologies and services to the public."

Finally, Section 107(b)(5) directs the Commission to "provide a reasonable time and conditions for compliance with and the transition to any new standard, including defining the obligations of telecommunications carriers * * * during any transition period." 47 U.S.C. § 1006(b)(5). As discussed above, the government believes that carriers that intend to meet their obligations under Section 103 by complying with the J-Standard should be required to implement the prescribed modifications to the J-Standard no later than 18 months after the modifications are required to have been adopted, meaning no later than 24 months after the Commission's Report and Order if the Commission remits the standard-setting task to TR45.2 under the proposed 180-day timetable (see pp. 29-30 supra). We do not contemplate that the Commission will subject carriers to any interim implementation obligations during the "transition period" preceding that deadline.

B. Party Join/Hold/Drop Information

1. The J-Standard does not require carriers to provide any message or signaling information indicating that a party has joined a multi-party call, been placed on hold, or dropped from the call. The Commission has tentatively concluded that the J-Standard is deficient in this regard and must be modified to ensure that carriers provide law enforcement with "reasonably available" party join,

party hold, and party drop information. Notice ¶¶ 85-86. The Commission has requested comments on this tentative conclusion.

The government agrees that Section 103(a)(2) of CALEA obligates carriers to provide law enforcement with reasonably available party join/hold/drop information. For reasons presented in our previous filings and noted by the Commission (Notice ¶ 85), party join/hold/drop information fits squarely within CALEA's definition of "call-identifying information," which includes dialing and signaling information that identifies the "origin, direction, destination, or termination of each communication generated or received by a subscriber" (47 U.S.C. § 1001(2) (emphasis added)). See Government Petition at 44-45; Government June Reply Comments at 53. As a practical matter, party join, party hold, and party drop information enables law enforcement to follow the course of multi-party calls and to determine who is participating in such calls at any particular time. Without such information, law enforcement often would not know who joins or leaves a conference call, whether the subject alternated between legs of the call, or which parties may have heard or said particular communications during the course of the call. See Notice ¶ 85.

As the Commission notes (Notice ¶ 86), a carrier's obligation to provide party join/hold/drop information, like its obligation to provide other kinds of call-identifying information, applies to information that is "reasonably available" to the carrier. For reasons given above, the Commission need not and should not use this standard-setting proceeding to determine whether party join/hold/drop information is reasonably available to particular carriers or platforms. Instead, the Commission should frame an appropriate definition of "reasonably available" and leave the application of that definition to be worked out by individual carriers and law enforcement on a case-

by-case basis. See pp. 18-20 supra. This observation applies with equal force to the other items of call-identifying information discussed below.

The Commission has tentatively concluded that a carrier is obligated to provide party join/hold/drop information only when the carrier's own facilities, equipment, or services are involved in providing the service (and hence network signals associated with the change in party status are generated). Notice ¶ 86. The Commission has tentatively concluded that a carrier is not obligated to provide such information when changes in party status are handled by customer premises equipment because, "from the carrier's point of view, the call's status is unchanged" in such cases. Ibid. The government agrees with this tentative conclusion. If a carrier's network is not "aware" of a party join, hold, or drop because the change is handled by customer premises equipment, law enforcement does not expect the carrier to provide notice of the change. See Government June Reply Comments at 52 n.30.

2. TIA has suggested previously that party join/hold/drop information is already substantially available to law enforcement under the J-Standard. See Notice ¶ 86 (discussing TIA's submission). Specifically, TIA has suggested that the information covered by the government's proposed Party Join message is provided by the J-Standard's Change message (acting in conjunction with the Origination and TerminationAttempt messages), and that the information sought by the proposed Party Drop message is provided by the J-Standard's Release message. See CC Docket No. 97-213, TIA Comments at 52-53 (filed May 20, 1998). The Commission has invited comments on this suggestion. Notice ¶ 86.

The government has addressed TIA's suggestion in earlier filings. See Government June Reply Comments at 51-52. As we have explained before, an examination of the J-Standard does not

support the suggestion. The J-Standard's Change message is not a substitute for party join information because the Change message is triggered by changes in call identities, rather than by changes in party identities, and therefore will not identify party joins if a manufacturer uses a single call identity to cover multiple legs of a call. Id. at 48-49, 51-52. As for party drops, the J-Standard's Release message is not a proxy for a party drop message because the J-Standard does not require a carrier to send the Release message when a single call leg or call appearance is released; instead, it makes the delivery of the Release message for such events discretionary. Government June Reply Comments at 52. Finally, we note that TIA has not suggested that the J-Standard provides any message that notifies law enforcement of party holds. In short, the J-Standard's existing messages cannot reasonably be claimed to substitute for the party join, hold, and drop information that Section 103(a)(2) of CALEA requires carriers to provide.

3. Requiring carriers to provide party join/hold/drop information is consistent with the statutory criteria of Section 107(b). For the reasons given above and in our earlier filings, party join/hold/drop information must be provided in order for carriers to "meet the assistance capability requirements" of Section 103, and carriers and manufacturers will be free to implement this capability by whatever specific technical means prove to be most "cost-effective" for them. 47 U.S.C. § 1006(b)(1). If individual carriers believe that providing party join/hold/drop information will be prohibitively expensive for them, they may seek relief under Section 109(b) of CALEA, which provides the Commission with a suitably tailored mechanism for making carrier-specific assessments of cost and other relevant criteria regarding "reasonable achievability" (see pp. 9-10 supra).

Requiring carriers to provide party join/hold/drop information will not impair "the privacy and security of communications not authorized to be intercepted." 47 U.S.C. § 1006(b)(2). To the contrary, this information may actually serve to enhance privacy. To the extent that receipt of party join/hold/drop information permits law enforcement to identify promptly the participants to a multi-party call, it may permit law enforcement to minimize surveillance of non-criminal conversations more quickly.

Requiring carriers to provide party join/hold/drop information should not have a material impact on residential ratepayers (47 U.S.C. § 1006(b)(3)) and should not affect "the provision of new technologies and services to the public" (*id.* § 1006(b)(4)). Finally, with respect to an implementation timetable (*id.* § 1006(b)(5)), we contemplate that this capability, like the other capabilities identified in the government's rulemaking petition, would be required to be implemented within 24 months of the Commission's Report and Order if the Commission provides for TR45.2 to adopt revised standards within 180 days (see pp. 29-30 *supra*).

C. Subject-Initiated Dialing and Signaling Information

1. During the course of a call that is subject to authorized electronic surveillance, an intercept subject may invoke services like three-way calling and call transfer by pressing feature keys or the flash hook. The J-Standard does not require carriers to provide a call data message when the subject inputs dialing or signaling information within a call in this fashion.

The Commission has tentatively concluded that subject-initiated dialing and signaling information constitutes "call-identifying information" for purposes of CALEA (Notice ¶ 91) and therefore must be provided to law enforcement when it is "reasonably available" to the carrier (Notice ¶ 94). The government agrees with this tentative conclusion. For reasons explained in our

earlier filings, when a subject presses a feature key or the flash hook to invoke features like three-way calling, call waiting, and call forwarding, the resulting dialing and signaling information identifies (depending on the particular feature involved) the "origin," "direction," "destination," and/or "termination" of each communication. See Government June Reply Comments at 46-48. Moreover, whenever the subject uses feature keys or the flash hook to control a call, he is engaged in the "direction" of his communications. Cf. 47 U.S.C. § 1002(a) (assistance capability requirements apply to all equipment, facilities, and services that allow subscriber to "originate, terminate, or direct communications") (emphasis added). The remote operation of these features (Notice ¶ 91) should not lead to a different result. However, we agree with the Commission that, insofar as these features are controlled by customer premises equipment and no network signal is generated, the dialing and signaling information will not be available to the carrier and therefore need not be provided by the carrier under Section 103(a)(2). See Government June Reply Comments at 49.

2. The Commission has noted that some commenters have asserted that the subscriber-initiated dialing and signaling information sought by the government is already provided in substantial part by the J-Standard. Notice ¶ 94. For example, TIA has asserted that, with respect to signaling activity that is transmitted from the subject to the network and detected by the switch, the J-Standard already provides law enforcement with "all potentially relevant call-identifying information." CC Docket No. 97-213, TIA Comments at 48-49.

These assertions are mistaken, for much the same reasons that TIA's similar assertions regarding party join and party drop information are mistaken (see pp. 46-47 supra). TIA's argument is based primarily on the operation of the J-Standard's Change message. But as discussed in our

prior filings (see Government June Reply Comments at 48-49), and as reviewed above, the Change message is tied to changes in call identity rather than party identity, and therefore will not necessarily disclose the use of feature keys and hook flashes that change the parties to a particular conversation within a multi-party call. For example, depending on how a particular manufacturer chooses to implement the J-Standard, a subject could press the flash hook to move back and forth repeatedly between two legs of a call without ever generating a Change message.

3. In the course of discussing subject-initiated dialing and signaling information, the Notice discusses the relationship between subject signaling and voice mail. Notice ¶ 93. The Notice states that "signaling data indicating that the subject is accessing his/her voice mail is properly classified as 'call-identifying information.'" Ibid. However, the Notice states that "[t]he contents of the voice mail * * * fall outside the scope of CALEA" because CALEA "does not apply to information services." Ibid. The first statement is correct, but the second statement requires qualification.

As the Commission is aware, Section 103(a)'s assistance capability requirements apply to "telecommunications carriers," and CALEA defines "telecommunications carrier" to exclude "persons or entities insofar as they are engaged in providing information services." 47 U.S.C. §§ 1001(8)(C)(i), 1002(a). CALEA's definition of "information services" includes voice mail services. See id. § 1001(6). Accordingly, "[t]he storage of a message in a voice mail or E-mail 'box' is not covered * * * ." House Report at 23, reprinted in 1994 USCCAN at 3503 (emphasis added). However, when a carrier redirects an incoming communication to a voice mail box, "[t]he redirection of the voice mail message to the 'box' * * * [is] covered," meaning that the carrier would have to provide the message to law enforcement in the course of the redirection (assuming, as always, that law enforcement has the necessary legal authorization to intercept the communication). Ibid.; see

also id. at 20, reprinted in 1994 USCCAN at 3500 ("the call redirection portion of a voice mail service [is] covered"). Conversely, when the subscriber signals the carrier to deliver a voice mail message to the subscriber's terminal, and the carrier transmits the message to the subscriber using the subscriber's equipment, facilities, and services, that transmission is likewise covered by Section 103(a). Thus, it is too broad to say that "the contents of the voice mail" fall outside the scope of CALEA: stored voice mail is not covered by CALEA, but the transmission of communications to and from voice mail boxes over a subscriber's "equipment, facilities, and services" is covered.

4. Requiring carriers to provide law enforcement with reasonably available subject-initiated dialing and signaling information is consistent with the criteria of Section 107(b) of CALEA. This capability must be added to the J-Standard in order to "meet the assistance capability requirements" of Section 103, and carriers and manufacturers are free to choose the most "cost-effective methods" for providing this information. 47 U.S.C. § 1006(b)(1). With respect to protecting the privacy and security of communications not authorized to be intercepted, minimizing the cost of compliance on residential ratepayers, and encouraging the provision of new technologies and services to the public (id. § 1006(b)(2)-(4)), this capability stands in much the same position as the capability to provide party join, hold, and drop information (see pp. 47-48 supra). Finally, the 24-month implementation period proposed above should be adequate to permit development, installation, and deployment of any network modifications required to provide this capability.

D. In-Band and Out-of-Band Network Signaling

1. When a call attempt is made to or from a subscriber's equipment, facilities, or services, the carrier's network generates in-band or out-of-band signals that identify call progress. These signals may be presented to the subject as audible tones, visual indicators, or alphanumeric display

information. For outgoing call attempts, these signals indicate (for example) whether the call attempt ended with a busy signal, ringing, or before the network could complete the call. For incoming call attempts, these signals indicate (for example) whether the subject's telephone received a call waiting tone or was alerted to the redirection of a call to voice mail by a "stutter" tone or a message-waiting indicator. Collectively, these signals show how the network treated a call attempt: whether or not it was completed, how the call may have been redirected or modified, and how the call ended.

The J-Standard does not require carriers to provide law enforcement with notification of network-generated in-band and out-of-band signaling relating to call progress. The Commission has tentatively concluded that certain types of in-band and out-of-band network signaling, such as notification that a voice mail message has been received by a subject, constitute "call-identifying information" under CALEA. Notice ¶ 99. The Commission suggests that there may be other types of in-band and out-of-band signaling information that would constitute call content rather than call identifying information. Ibid. However, the Commission correctly notes that CALEA requires carriers to provide law enforcement both with call content and with call-identifying information, and the Commission therefore does not propose to decide what network signaling information falls into which category "[u]nless necessary to establish technical standards under CALEA's safe harbor." Ibid. The Commission requests comments regarding "what types of in-band and out-of-band signaling" must be provided to meet the assistance capability requirements of Section 103. Ibid.

The government's rulemaking petition identifies the specific kinds of network-generated notification signals that the government believes to be required by Section 103. See Government Petition, Appendix 1 (§ 64.1708(d)). The basic object is to receive network signals that report the

progress of outgoing and incoming call attempts. Specifically, the government seeks delivery of a notification message when the accessing system sends an audible in-band signal to the subscriber (such as a busy signal) or sends an out-of-band signal to the subscriber's terminal to activate, deactivate, or control the following indications of incoming calls or messages:

- Any alerting of incoming calls or messages;
- Audible indications of incoming calls or messages;
- Visual indications of incoming calls or messages, such as lights indicating call waiting; and
- Alphanumeric display information, such as messages sent to the terminal, calling number identification, or calling name identification.

In our view, all of this information constitutes "call-identifying information," because it identifies the "termination" (and, in some instances, the "direction" or "destination") of a communication. See Government Petition at 45-46; Government June Reply Comments at 55-56. As a result, the J-Standard's failure to require carriers to deliver such information renders it deficient.⁷ We do not believe that any of this information constitutes call content, but even if it did, that would not make the J-Standard any less deficient, since (as the Commission points out) Section 103 obligates carriers to provide law enforcement with all call content as well as call-identifying information. Indeed, a carrier's obligation to deliver call content under Section 103(a)(1) is even broader than its obligation to deliver call-identifying information under Section 103(a)(2), since Section 103(a)(1) is not restricted to call content that is "reasonably available" to the carrier.

⁷ TIA has asserted previously that the J-Standard provides much of the information that the government is seeking through this punch list capability. We have responded to that assertion in our earlier filings. See Government June Reply Comments at 57-59.

2. Requiring carriers to deliver network-generated in-band and out-of-band signaling information to law enforcement is consistent with the statutory criteria of Section 107(b) of CALEA. For reasons given above and in our earlier filings, delivery of network-generated signaling information is necessary to "meet the assistance capability requirements" of Section 103 and may be carried out by "cost-effective methods." 47 U.S.C. § 1006(b)(1). If network signaling information is delivered to law enforcement over a call data channel, as the government has proposed, the "the privacy and security of communications not authorized to be intercepted" (id. § 1006(b)(2)) will be enhanced by preventing the risk of inadvertent intrusions on call content in pen register cases. See Government Petition at 48. We are aware of no reason why delivery of this information would materially affect residential ratepayers or would impede the provision of new technologies and services to the public. 47 U.S.C. § 1006(b)(3)-(4). Finally, it should be possible for carriers to implement this capability within the 24-month period discussed above (see pp. 29-30 supra).

E. Timing Requirements

Section 103(a)(2) of CALEA obligates carriers to provide law enforcement with access to call-identifying information "before, during, or immediately after the transmission of a wire or electronic communication," and "in a manner that allows it to be associated with the communication to which it pertains." 47 U.S.C. § 1002(a)(2)(A)-(B). Despite these requirements, the J-Standard does not contain any provision obligating carriers to deliver call-identifying information in a timely fashion, nor does it contain any provision requiring carriers to provide information about the time that call events actually occurred. As a result, as matters now stand, a carrier that delivers call-identifying information to law enforcement is in compliance with the J-Standard even if it delivers

the information long after a communication is over, and even if law enforcement is unable to associate particular call-identifying information with particular communications because it lacks accurate information about when the call events occurred.

The Commission has tentatively concluded that the J-Standard must be modified to require carriers to deliver call-identifying information within a "reasonable amount of time" and to "stamp" call-identifying information with the time of the underlying call event. Notice ¶ 104. The government agrees with this tentative conclusion. By its terms, Section 103(a)(2) requires carriers to isolate call-identifying information "expeditiously" and to provide such information to law enforcement "before, during, or immediately after the transmission of a wire or electronic communication." 47 U.S.C. § 1002(a)(2)(A). An industry standard that places no time limit whatsoever on the delivery of call-identifying information is patently inconsistent with this requirement. And as the Commission has pointed out (Notice ¶ 104), time stamping is necessary to allow law enforcement agencies to "associate[] [call-identifying information] with the communication to which it pertains" (47 U.S.C. § 1002(a)(2)(B)), particularly when a subject makes or receives a series of calls within a short time. Ibid.

The Notice suggests that time stamp information -- for example, the information that a subject hung up at 1:23:00.00 AM -- is itself "call-identifying information." See Notice ¶ 104. Although it is possible to read the statutory definition of call-identifying information to encompass information about the timing of a communication's "origin, direction, destination, or termination" (47 U.S.C. § 1001(2)), the government's time stamp proposal does not require such a reading. Whether or not a time stamp is itself call-identifying information, information about the timing of call events must be provided to ensure that call-identifying information can "be associated with the

communication to which it pertains," as required by Section 103(a)(2)(B) of CALEA (47 U.S.C. § 1002(a)(2)(B)). The government therefore invites the Commission to predicate any time stamp requirement in its Report and Order on Section 103(a)(2)(B)'s "association" requirement, as well as (or in lieu of) classifying time stamp information as "call-identifying information."

2. To give practical content to the general timing requirements of Section 103(a)(2), the J-Standard must be modified to incorporate specific timing provisions. In its rulemaking petition, the government has proposed that time stamps be accurate to within 100 milliseconds and that call event messages be delivered within 3 seconds (99 percent of the time). See Government Petition, Appendix 1 (§ 64.1708(e)). The Commission has requested comments on the technical feasibility of these proposals.

The government does not believe that there are any technical reasons why carriers cannot meet these (or comparable) timing requirements. The specific delivery time proposed in the government's rulemaking petition (within 3 seconds of the associated call event) was selected to make compliance feasible for a wide range of carriers utilizing a variety of platforms. The vast majority of carriers routinely deliver signaling information for call setup and takedown purposes in well under three seconds -- commonly in a matter of milliseconds. And by requiring only 99 percent reliability, the proposed delivery requirement accommodates the possibility of network congestion. The government is not asking carriers to process call-identifying information for CALEA purposes any more rapidly than carriers handle such information for their own call processing purposes.

As the Commission has pointed out (Notice ¶ 104), Section 103(a)(2) does not specify particular timing requirements. The government therefore does not contend that the specific timing provisions discussed above are the only possible ones that would satisfy the requirements of Section

103(a)(2). But the J-Standard must be modified to incorporate some timing requirements in order to give effect to the general timing provisions of Section 103(a)(2), just as the J-Standard designates specific call-identifying information messages and message parameters (see J-STD-025 §§ 5.4.1-5.4.10, 6.3.1-6.3.10, 6.4.1-6.4.11) to give effect to CALEA's general definition of "call-identifying information." It therefore will not do for carriers to argue that it is "arbitrary" to incorporate specific timing requirements into the J-Standard. As we have noted before, the whole point of the standard-setting process is to give specific content to the general provisions of Section 103 by identifying precisely what steps are required for a carrier to meet its underlying assistance capability obligations.

3. The timing requirements proposed above are consistent with the statutory criteria of Section 107(b) of CALEA. For the reasons given above and in our earlier filings, timing requirements are necessary to "meet the assistance capability requirements" of Section 103. 47 U.S.C. § 1006(b)(1). The Commission is not being called upon to prescribe how those requirements are to be implemented with respect to any particular platform, leaving manufacturers and carriers free to implement the requirements by the most "cost-effective methods" available to them. Ibid. Requiring accurate time stamps and timely delivery of call-identifying information will not harm "the privacy and security of communications not authorized to be intercepted" (id. § 1006(b)(2)); to the contrary, they have the potential to protect privacy interests by assisting law enforcement in minimizing the interception of non-criminal conversations. These timing requirements should not materially affect the costs borne by residential ratepayers and should not interfere with "the provision of new technologies and services to the public." Id. § 1006(b)(3)-(4). And the implementation period proposed above (see pp. 29-30 supra) should be more than sufficient to allow manufacturers

and carriers to make any modifications needed to implement the specific timing requirements prescribed by the Commission (*id.* § 1006(b)(5)), particularly since carriers are not being asked to process call-identifying information more rapidly for CALEA purposes than for their own call processing purposes.

F. Surveillance Integrity

1. The government's rulemaking petition includes three specific capabilities that address the need for "surveillance integrity" -- the need for the carrier to take concrete measures to ensure that its equipment, facilities, and services are capable of delivering authorized communications and call-identifying information to law enforcement (see 47 U.S.C. § 1002(a)(1)-(2)) and the corresponding need for the carrier to protect "the privacy and security of communications and call-identifying information not authorized to be intercepted" (see *id.* § 1002(a)(4)(A)). See Government Petition at 52-57 and Appendix 1 (§ 64.1708(f)-(h)). The Commission has tentatively concluded that the J-Standard does not have to be modified to incorporate any of the capabilities covered by these punch list items. See Notice ¶¶ 109, 114, 121. The government respectfully disagrees with this tentative conclusion. The government does not contend that the specific surveillance integrity mechanisms proposed in the government's rulemaking petition are mandated by Section 103 of CALEA. But Section 103 obligates carriers to take some affirmative steps to ensure surveillance integrity, and the J-Standard excuses carriers from taking any such steps. The Commission must correct that deficiency.

As the Commission is aware, the government believes that the J-Standard falls short in three specific respects in terms of surveillance integrity. First, the J-Standard does not obligate carriers to take any steps to ensure that authorized surveillance is "up and running" within the carrier's

network and that the carrier is accessing the call content and call-identifying information of the correct subscriber. Through human or mechanical error, a carrier may fail to initiate an interception or may inadvertently access the communications of the wrong subscriber. When this happens, law enforcement will not obtain the communications to which it is entitled, and if the interception is directed at the wrong subscriber, the privacy of communications to which law enforcement is not entitled will be inadvertently compromised. Yet the J-Standard places a carrier under no obligation to monitor an interception (or to provide law enforcement with the means to monitor it) to safeguard against such errors.

Second, the J-Standard does not require carriers to employ any mechanism to ensure that the channels used to deliver intercepted call content from the carrier to law enforcement are in working order. If the connection between the carrier and law enforcement is physically broken or otherwise interrupted, potentially critical and irreplaceable evidence of criminal activity may be lost. Law enforcement agents monitoring the subscriber's calls will hear nothing, but in the case of an analog connection, they will have no way of knowing whether silence means that the connection is broken or instead that the subscriber is simply not using his phone. The J-Standard nevertheless does not require carriers to take any steps to ensure that the connection is operational or to enable law enforcement to detect interruptions in a timely manner.

Third, the J-Standard has no mechanism for ensuring that law enforcement is notified of changes in a subscriber's features and services that could affect the provisioning of the interception.

When a subscriber adds or changes features and services like call forwarding, call waiting, and conference calling, law enforcement may have to make corresponding changes in the number of delivery channels in order for the intercepted communications actually to be delivered to law

enforcement. If law enforcement is unaware of the subscriber's actions, the interception will not be adequately provisioned and critical evidence may be lost. Yet the J-Standard does not require a carrier to take any steps to alert law enforcement of feature and service changes that could lead to this kind of loss.

In our view, the language of Section 103 requires affirmative measures by carriers in each of these three respects, and the J-Standard is deficient as a legal matter in not requiring carriers to employ any such measures. By its terms, Section 103 requires carriers to "ensure" that their communications equipment, facilities, and services are capable of expeditiously isolating and delivering to law enforcement, "to the exclusion of any other communications," "all communications" to or from the "equipment, facilities, or services of a subscriber * * * ." 47 U.S.C. § 1002(a)(1). Section 103 further requires carriers to "ensure" that their equipment, facilities, and services are capable of expeditiously isolating and delivering to law enforcement all "reasonably available" call-identifying information. Id. § 1002(a)(2). At the same time, Section 103 requires carriers to "ensure" that their equipment, facilities, and services are capable of implementing authorized electronic surveillance "in a manner that protects * * * the privacy and security of communications and call-identifying information not authorized to be intercepted." Id. § 1002(a)(4).

Simply stated, a carrier that does not take any affirmative steps to monitor the integrity of authorized electronic surveillance is not "ensuring," as Section 103 requires, that its equipment, facilities, and services are capable of delivering "all communications" and all reasonably available call-identifying information that law enforcement is authorized to intercept while protecting the privacy and security of other communications and call-identifying information. As law enforcement agencies have learned through decades of experience, electronic surveillance cannot be relied on to

provide all of the communications covered by a given surveillance order, while excluding other communications, unless ongoing steps are taken to provide assurance of the surveillance's integrity. Thus, surveillance integrity features of the sort that we have proposed do not constitute mere "quality control" measures (Notice ¶ 121); to the contrary, they are essential components of compliance with Section 103. Nor does the absence of these features, or similarly effective alternative measures, merely prevent a carrier's compliance with § 103 from being "proven or verified on a continual basis" (Notice ¶¶ 109, 114); rather, these deficiencies mean that carriers implementing the J-Standard will not be complying with the mandates of Section 103 in the first instance.

By way of analogy, we invite the Commission to imagine a statute that requires air carriers to "ensure" that their planes are capable of delivering "all" passengers safely to their destinations. Cf. 49 U.S.C. § 44705(1) (air carrier operating certificate "shall contain terms necessary to ensure safety in air transportation"). Suppose that a particular carrier has a fleet of planes that have the technical capability to transport the carrier's passengers among the various cities served by the carrier. However, the planes do not have automated systems to detect particular in-flight mechanical or electrical problems, and the carrier does not require its pilots to check for such problems in any other fashion. The planes do not have automated systems to report deviations from the plotted route, and the carrier does not require its pilots to monitor the route once the course has been set. Finally, when unexpected changes in passenger load cause the carrier to switch from a small plane to a larger plane, the carrier does not provide notice to the destination airport, which needs to make a corresponding change in runways to handle the larger plane.

It is possible that this air carrier could operate for some period without an accident. But it hardly would follow that the carrier was meeting its statutory obligation to "ensure" that its planes

were capable of delivering all of its passengers safely. It would be no answer for the carrier to say that its planes have the range and size needed to deliver its passengers to their destinations; a law requiring the carrier to "ensure" safe delivery of all passengers obviously requires something more. And while the carrier might be able to ensure safe delivery without using a particular safety mechanism, such as (for example) automated notification of course deviations, it would remain incumbent on the carrier to employ some affirmative mechanisms to ensure that all of its passengers will actually reach their destinations safely.

In the government's view, a telecommunications carrier that does not take any affirmative steps to "ensure" the integrity of authorized electronic surveillance is in the same position as the air carrier in the foregoing example. If a telecommunications carrier is to ensure (as Section 103 requires) that it is capable of delivering all communications and call-identifying information to law enforcement, while simultaneously protecting the privacy and security of communications and call-identifying information not authorized to be intercepted, it must take affirmative steps to make certain that the surveillance is up and running on the right subscriber; that the delivery channels from the carrier to law enforcement are working; and that the law enforcement agency is aware of changes in subscriber services that may require corresponding changes in the provisioning of the surveillance.

Without such steps, it is inevitable that carriers will fail to provide law enforcement with all of the communications and call-identifying information to which law enforcement is entitled under Section 103 and underlying electronic surveillance statutes, and it is equally inevitable that carriers will occasionally deliver communications and call-identifying information to which law enforcement is not entitled. Yet the J-Standard does not require carriers to take any -- we repeat, any -- affirmative

steps in any of these regards. The complete omission of any affirmative surveillance integrity requirements in the J-Standard simply cannot be squared with Section 103.

The Commission should also recognize that the absence of surveillance integrity features in the J-Standard not only will lead to the loss of evidence that law enforcement is authorized to acquire, but also may limit the evidentiary value of the evidence that law enforcement does acquire. Criminal defendants challenging the use of electronic surveillance seek to exploit every discernible weakness in electronic surveillance techniques, and it cannot have been Congress's intention in enacting CALEA to expand their opportunities to do so. Yet to the extent that a defendant can argue that law enforcement may not have intercepted all of his communications over the surveilled facilities during the intercept period, he can claim that law enforcement missed a crucial communication (or a portion of a communication) that would have exculpated him. It was to ensure that our use of electronic surveillance could not be undermined in this fashion that we have traditionally included surveillance integrity features in our intercepts, and it was to preserve and protect -- rather than to undermine -- our continued ability to use electronic surveillance in successfully prosecuting criminals that Congress enacted CALEA. The J-Standard's lack of any surveillance integrity features directly compromises this goal.

2. Whether the absence of surveillance integrity mechanisms renders the J-Standard deficient is, of course, a distinct question from how the deficiency should be corrected. If the Commission revises its tentative conclusion regarding the first question, it then must turn to the second one.

As the Commission is aware, the government has proposed that carriers ensure surveillance integrity through the automated delivery of surveillance integrity messages. Specifically, we have proposed that carriers deliver: (1) a surveillance status message, which would periodically verify that

the intercept is accessing the correct equipment, service, or facility; (ii) a continuity tone, which would verify that the call content channels between the carrier and law enforcement are in working order; and (iii) a feature status message, which would report specific changes in a subscriber's calling features and services. See Government Petition, Appendix 1 (64.1708(f)-(h)).

In proposing the automated delivery of this information to law enforcement, we should not be understood to be claiming that the information qualifies as "call-identifying information." To the contrary, we agree with the Commission's tentative conclusion that the information in question is not call-identifying information. See, e.g., Notice ¶ 121 (feature status messages "do not constitute call-identifying information"). The government seeks this information not because the information is itself call-identifying information, but rather because delivery of the information -- or some other, equally effective affirmative measure -- is necessary for a carrier to meet its statutory obligation of "ensuring" that law enforcement receives the communications it is entitled to receive while the privacy and security of other communications is protected.

In our view, each of the proposed punch list items relating to surveillance integrity satisfies the statutory criteria of Section 107(b) of CALEA. To begin, for the reasons given above and in our earlier filings, affirmative steps to ensure surveillance integrity are necessary to "meet the assistance capability requirements" of Section 103. 47 U.S.C. § 1006(b)(1). The automated delivery of surveillance status messages, feature status messages, and continuity checks will realize that goal. Moreover, automated delivery of this information, rather than reliance on manual alternatives that require human intervention and monitoring by carrier personnel, represents a "cost-effective method" (*ibid.*) of accomplishing that goal. Our discussions with industry have indicated that the cost of implementing a continuity check (such as a C-tone) would be trivial, and we anticipate that periodic

automated delivery of surveillance status messages and feature status messages likewise would not involve significant expense.

The automated delivery of surveillance integrity information is also consistent with the goal of "protect[ing] the privacy and security of communications not authorized to be intercepted." 47 U.S.C. § 1006(b)(2). Indeed, as indicated above, the automated delivery of a surveillance status message will affirmatively enhance legitimate privacy interests, by promptly alerting law enforcement if a carrier has inadvertently directed the surveillance toward the wrong subscriber.⁸

Because the cost of delivering automated surveillance integrity messages should be relatively minor, implementing these features should not have a material impact on residential ratepayers. 47 U.S.C. § 1006(b)(3). And we see no way in which the implementation of these features could reasonably be claimed to impede "the provision of new technologies and services to the public." *Id.* § 1006(b)(4). Finally, with respect to the need for transition provisions (*id.* § 1006(b)(5)), there is no reason why these features cannot be implemented within the general 24-month implementation period proposed above (see pp. 29-30 *supra*).

As we have previously stated, we are not arguing that the automated messages proposed in the government's rulemaking petition are the only possible means of ensuring surveillance integrity under Section 103. See Government Petition at 53-54; Government June Reply Comments at 67, 72. We reiterate that point here. Although we continue to believe that automated messages are an appropriate and effective means of implementing Section 103, we acknowledge that there may be

⁸ The Commission has asked whether a continuity tone "could * * * be detected by the subscriber whose facilities are under surveillance." Notice ¶ 115. It could not. The tone would be applied solely to the channel delivering call content to law enforcement.

other means by which a carrier might meet its assistance capability obligations in these regards. But the Commission should not excuse carriers from having to implement any affirmative measures to ensure surveillance integrity if the Commission concludes that the particular measures proposed by the government are not mandated by Section 103 or are otherwise inappropriate. If the J-Standard is deficient in this respect, the deficiency must be corrected -- if not by the means proposed by the government, then by some other, equally effective means.

G. Post-Cut-Through Dialing

1. In long distance calls, credit card calls, and (in some instances) local calls, the dialing and signaling information necessary to route the call to the intended party may occur after the call has been initially "cut through" by the originating carrier. See Government Petition at 38-39 & n.16. In these cases, the destination of the call is revealed only by the numbers dialed after the cut-through. Under the J-Standard, however, originating carriers are not obligated to provide law enforcement with access to post-cut-through dialing. Instead, law enforcement receives only the digits dialed before cut-through, such as the numbers dialed to access a "1-800" long distance service -- numbers that ordinarily have no value to law enforcement whatsoever.

The Commission has tentatively concluded that "post-cut-through digits representing all telephone numbers needed to route a call * * * are call-identifying information." Notice ¶ 128. The government agrees with that tentative conclusion. CALEA defines "call-identifying information" to include "dialing or signaling information that identifies the * * * destination * * * of each communication generated * * * by a subscriber." 47 U.S.C. § 1001(2). Post-cut-through digits that are used for call routing fit squarely within this statutory definition. CALEA's definition of "call-identifying information" conspicuously does not add a further requirement that such information be

used by the originating carrier, as distinct from some other carrier, for call routing purposes. As a result, the fact that originating carriers transmit post-cut-through digits over a call content channel, rather than a call data channel, does not mean that post-cut-through dialing "should be treated as content for purposes of CALEA" (Notice ¶ 128).

2. The Commission has asked for comments on how post-cut-through dialing can be extracted from the call content channel by the originating carrier for delivery to law enforcement. Notice ¶ 128. In the absence of an "out-of-switch" solution, such as implementation of SS7's option for returning the number of the answering party to the originating carrier (see Government June Reply Comments at 43 n.25), we anticipate that the originating carrier's hardware will have to be modified in order to detect and extract post-cut-through digits. To capture post-cut-through digits for delivery to law enforcement, an originating carrier may apply a tone decoder to the call or may detect the dialed digits outside the switch by a "loop-around" or other means.

In a related vein, the Commission has asked for comments on whether post-cut-through digits used for call routing can be "distinguished" from other post-cut-through dialing. Notice ¶ 128. We assume that the Commission is interested in the ability of originating carriers to "distinguish" between these two types of post-cut-through dialing by automated, real-time means, permitting carriers to deliver to law enforcement only those post-cut-through digits that are used for call routing. As far as the government is aware, that technical capability does not currently exist. Post-cut-through dialing for call routing purposes currently can be distinguished from post-cut-through dialing for other purposes only by "manual" means (that is, human review). If originating carriers did have the technical ability to perform this function on an automated, real-time basis, law enforcement would have no objection to (and indeed would welcome) such an approach.

3. The Commission has asked for comments on whether post-cut-through dialed digits are "reasonably available" (47 U.S.C. § 1002(a)(2)) to originating carriers. Notice ¶ 128. The Commission notes in this regard that industry and privacy groups have expressed concern about the potential costs involved in "design[ing], build[ing], and incorporat[ing] [post-cut-through dialed digit extraction] into telephone network infrastructures." *Ibid.* The Commission seeks comments on whether "originating, intermediate, or terminating carriers can deliver such call-identifying information by cost-effective means." *Ibid.* The government offers the following comments regarding reasonable availability and cost.

First, for reasons set forth above, the government does not believe that cost considerations are germane to determinations of "reasonable availability" under Section 103(a)(2) of CALEA. See pp. 13-15 *supra*. And for the Commission to attempt to include or exclude particular capabilities categorically from the J-Standard on the basis of cost considerations would be particularly ill-advised. The Commission's standard-setting role under Section 107(b) is, and should be, aimed at the formulation of generally applicable standards for the entire class of carriers (wireline, cellular, and broadband PCS) that are subject to the J-Standard. The costs associated with post-cut-through dialed digit extraction, in contrast, can be expected to vary from platform to platform and carrier to carrier. For reasons given above, the appropriate mechanism for dealing with such individualized cost concerns is the "reasonable achievability" mechanism of Section 109(b) of CALEA, not the safe-harbor standard-setting mechanism of Section 107(b). See pp. 9-15 *supra*.

Second, it would not be cost-effective to look to intermediate carriers or terminating carriers, rather than originating carriers, to provide law enforcement with post-cut-through dialing. In order for an intermediate carrier to capture post-cut-through dialing covered by a pen register order and

deliver the dialed digits to law enforcement "before, during, or immediately after the transmission" of the call (47 U.S.C. § 1002(a)(2)(A)), the intermediate carrier would have to monitor every incoming call that it receives in order to determine whether the call originated from the facilities of a subscriber covered by the order, and it would have to do so with respect to every outstanding pen register order in the country. Requiring a terminating carrier to capture and deliver post-cut-through digits would be equally burdensome: because an intercept subject could call any subscriber served by the terminating carrier, the terminating carrier would have to monitor every switch in its network. In contrast, the originating carrier only has to monitor the particular switches that are used to provide service to the particular subscriber whose facilities are under surveillance. There are still further practical problems, identified in our earlier filings, with requiring law enforcement to obtain post-cut-through dialed digits from carriers other than the originating carriers. See Government June Reply Comments at 41-42 & n.24.

Third, as we have noted above, the industry's proposed definition of "reasonably available" in the J-Standard would effectively excuse all originating carriers from providing access to post-cut-through dialing, even if doing so would not impose significant costs or technical obstacles, because post-cut-through digits are not present at the originating carrier's IAPs "for call processing purposes" (J-STD-025 § 4.2.1). We have already explained why the Commission should excise the "call processing purposes" restriction from the J-Standard's definition of "reasonably available." See pp. 23-24 supra. We simply remind the Commission here that failure to do so would effectively nullify the Commission's tentative conclusion that post-cut-through dialing is call-identifying information, and would make it far easier for criminals to evade authorized pen register surveillance.

4. Requiring originating carriers to provide post-cut-through dialed digits is consistent with the statutory criteria of Section 107(b). For the reasons outlined above and in our earlier filings, law enforcement must be provided with post-cut-through dialing used for call routing if the J-Standard is to "meet the assistance capability requirements" of Section 103. 47 U.S.C. § 1006(b)(1). Requiring originating carriers rather than other carriers to provide this information is a "cost-effective method" of implementing this capability, as discussed above. Ibid. Requiring originating carriers to extract dialed digits from post-cut-through call content "protect[s] the privacy and security of communications not authorized to be intercepted." Id. § 1006(b)(2). We cannot provide a specific estimate of the extent to which the cost of this capability will be borne by residential ratepayers, but we note again that Section 107(b)(3) provides for the Commission to "minimize the cost of * * * compliance" on residential ratepayers, not to absolve carriers from compliance because of such costs. 47 U.S.C. § 1006(b)(3). Requiring originating carriers to extract post-cut-through digits should not adversely affect "the provision of new technologies and services to the public" (id. § 1006(b)(4)), and we see no reason why this capability cannot be implemented within 24 months after revised technical standards are adopted pursuant to the Commission's Report and Order, if not sooner.

H. Delivery Interface

1. In order for call content and call-identifying information to be delivered from a carrier to a law enforcement agency, the parties must use a common delivery interface. Although the J-Standard contains non-binding information regarding the delivery protocols preferred by law enforcement (see J-STD-025, Annex A, §§ A.5-A.6 & Figures 23-25), it does not contain any limitation on the number of protocols that may be used by carriers to deliver call content and call-identifying information.

Section 103 does not obligate carriers to use any particular delivery interface, and the government has not asked the Commission to impose such an obligation. However, the government has asked the Commission to place a limitation on the number of interfaces employed by carriers under the J-Standard. See Government Petition 57-58 & Appendix 1 (§ 64.1708(j)). As explained in the Government Petition, a limit on the number of protocols is necessary to "ensure," as a practical matter, that all content and call-identifying information that carriers are obligated to provide can actually be delivered. Ibid. Unless a relatively small number of standardized protocols are employed, each carrier will be free to employ a different interface protocol, and law enforcement agencies could be faced with prohibitive practical and financial burdens in equipping themselves to deal with scores of different protocols. As a practical matter, law enforcement agencies thus would be denied access to information to which they are guaranteed access by CALEA.

The Government Petition therefore asks the Commission to limit the number of interfaces to no more than five for the delivery of call content (i.e., five CCC protocols) and five for the delivery of call-identifying information (i.e., five CDC protocols). See Government Petition, Appendix 1 (§ 64.1708(j)). Within this limit, industry should be free to determine for itself which protocols will be used. In proposing a limit of five protocols, we do not mean to suggest that five is the only reasonable limit. The adoption of some reasonable limit, however, is necessary to ensure that the assistance capability requirements of Section 103 are not rendered illusory in practice by a proliferation of differing protocols. The Commission therefore should determine that the J-Standard's failure to place a limit on the number of delivery interfaces renders it deficient and should require industry to select an appropriately limited number of protocols for use under the J-Standard.

2. Although the Government Petition asks the Commission to include a limit on the number of delivery interfaces as part of the Commission's Report and Order, the Notice does not express a tentative conclusion about the appropriateness of such a limit, nor does it seek comments on the issue. The omission of this issue from the Notice may reflect a perception on the part of the Commission that the government is no longer seeking to modify the J-Standard in this regard. See Notice ¶ 13 & n.30. If so, that perception is incorrect.

The Commission may have misunderstood the import of a letter from Assistant Attorney General Stephen R. Colgate to Mr. Tom Barba regarding CALEA's assistance capability requirements, a copy of which is attached as an appendix to the Government Petition. In that letter, Assistant Attorney General Colgate stated that "a single delivery interface is not mandated by CALEA." Government Petition, Appendix 5, p. 3 (emphasis added). The Colgate letter went on to explain that the government supported a compromise under which industry would employ "a limited number of no more than five delivery interfaces." Ibid.

The Notice implies that the Commission understands the Colgate letter to have dropped the subject of delivery interface protocols from the government's "punch list." See Notice ¶ 13 & n.30. That is not the case. The Colgate letter simply states that Section 103 of CALEA does not obligate industry to select "a single delivery interface." The letter does not suggest that carriers should therefore be free under the J-Standard to employ an unlimited number of delivery interface protocols. To the contrary, it urges the adoption of a specific limit on the number of protocols. The Government Petition, filed after the Colgate letter, reiterates that request. In short, the government continues to believe that a limitation on the number of delivery interface protocols is necessary in order to ensure the effective delivery of call content and call-identifying information under Section

103 of CALEA, and we renew our request for the Commission to include such a limitation in its Report and Order.

3. Imposing a limitation on the number of delivery interface protocols is consistent with the criteria of Section 107(b) of CALEA. For the reasons given above, limiting the number of delivery interfaces will ensure that industry "meet[s] the assistance capability requirements" of Section 103 and will do so "by cost-effective methods." 47 U.S.C. § 1006(b)(1). Placing a limit on the number of delivery interface protocols will not affect "the privacy and security of communications not authorized to be intercepted" and should not increase "the cost of * * * compliance on residential ratepayers." *Id.* § 1006(b)(2)-(3). Because the government's proposal would leave to industry itself the choice of which protocols to use, and because the proposal would impose no restriction on the choice of protocols for other (non-CALEA-related) network delivery functions, the proposal would not impair "the provision of new technologies and services to the public. *Id.* § 1006(b)(4). And because industry is free to select from existing delivery interface protocols, rather than having to develop new protocols, there is no need to provide for a special transition period or transitional obligations once industry has designated its preferred protocols pursuant to the Commission's Report and Order. *Id.* § 1006(b)(5).

III. Comments Regarding Other Capabilities

The Commission also has requested comments regarding two aspects of the J-Standard that have been called into question by CDT and other privacy groups. First, the J-Standard requires carriers to provide law enforcement with access to certain information regarding the location of mobile terminals when law enforcement is legally authorized to obtain such information. CDT contends that the J-Standard's location information provisions are invalid because location

information is not "call-identifying information." Second, when communications are transmitted using packet switching protocols, the J-Standard requires carriers to deliver the entire packet data stream associated with a given communication, including call content, except where information is not authorized to be acquired. CDT argues that when law enforcement lacks legal authority to intercept call content, Section 103(a)(4)(A) of CALEA (47 U.S.C. § 1002(a)(4)(A)) requires carriers to strip out call content from the packet data stream before delivering it to law enforcement. The Commission has tentatively rejected the first of these two objections and has asked for additional comments regarding the issues raised by the second objection. For reasons that we present below, we agree with the Commission's tentative conclusion regarding location information, and we do not believe that CALEA requires the Commission to modify the J-Standard's packet mode provisions in the manner urged by CDT.

A. Location Information

1. In certain circumstances, the J-Standard requires carriers to provide law enforcement agencies with location information at the beginning and end of communications to and from mobile terminals. See J-STD-025 § 5.4.1 (Answer Message parameters), § 5.4.5 (Origination Message parameters), § 5.4.6 (PacketEnvelope Message parameters), § 5.4.8 (Release Message parameters). The "Location" parameter is defined as a text string that "provides location information about the subject's mobile terminal." *Id.* § 6.4.6.

The Commission has tentatively concluded that location information is "call-identifying information" under CALEA. Notice ¶ 52. For reasons that we have previously presented to the Commission, we agree with that conclusion. As we have explained previously, location information comes within the general statutory definition of "call-identifying information" (47 U.S.C. § 1001(2)),

and Section 103(a)(2) of CALEA (47 U.S.C. § 1002(a)(2)) excludes location information from that general definition only in cases where a law enforcement agency is acquiring information "solely pursuant to the [statutory] authority for pen registers and trap and trace devices * * * ." See Government May Comments at 17-21; Government June Reply Comments at 78-79. We incorporate our earlier comments on this issue by reference here.

2. The Notice states that the J-Standard is "unclear" regarding the degree of specificity required for location information. Notice ¶ 54. The Commission has tentatively concluded that "location information should be construed [in the J-Standard] to mean cell site location at the beginning and end of the communication." Id. ¶ 55. The Notice requests comment on this tentative conclusion.

We agree that the J-Standard requires a carrier only to have the capability to supply cell site information (or comparably specific location information), and only at the beginning and termination of the call. This means that a carrier that has the capability of supplying cell site information is in compliance with this part of the J-Standard and, hence, in compliance (in this respect) with Section 103 of CALEA. See Government May Comments at 19. A carrier need not have the capability to deliver more detailed location information in order to satisfy its obligations under the J-Standard and CALEA.⁹

⁹ While CALEA does not require carriers to deliver more extensive location information than that specified by the J-Standard, neither does CALEA prohibit them from delivering more extensive location information when: (1) they have designed their networks to generate such information; and (2) law enforcement has been legally authorized by a court to obtain such information. In relatively rare cases, where law enforcement has shown that precise location information is vital to a criminal investigation, courts have ordered wireless carriers who possess such information to provide it to law enforcement. The delivery of such information is entirely consistent with Section 103(a)(4)(A) of
(continued...)

3. The Commission has tentatively concluded that the location information required by the J-Standard is "reasonably available." Notice ¶ 56. While determinations of "reasonable availability" may vary among carriers and platforms (see pp. 18-19 supra), this tentative conclusion is likely to be correct as a general matter. As the Notice points out, location information is already available to wireless carriers in connection with billing, hand-off, and system use features. Ibid. And as the Notice points out, carriers will also be required to have location information capabilities by the E911 initiative. Ibid. As a result, the location information covered by the J-Standard should be "reasonably available" to wireless carriers even under the existing definition of "reasonably available" in the J-Standard, and a fortiori, such information should be "reasonably available" if that definition is modified in the respects that we have proposed (see pp. 20-25 supra). In response to the Commission's request for comments on "how the Commission should decide or interpret the term 'reasonably available' in the context of the proposed location information requirement" (Notice ¶ 56), we do not believe that there is any need for the Commission to interpret or construe "reasonable availability" differently in connection with location information than in connection with the other kinds of call-identifying information at issue in this proceeding.

4. Because the J-Standard's location information provisions do not render the J-Standard deficient, the Commission need not address the statutory criteria in Section 107(b), which are directed at determining how deficiencies in industry standards are to be redressed. We note,

⁹(...continued)

CALEA, which obligates carriers to protect "the privacy and security of communications and call-identifying information not authorized to be intercepted" (47 U.S.C. § 1002(a)(4)(A)), because the information will be provided only when it is "authorized to be intercepted." We repeat, however, that CALEA does not obligate carriers to design their networks to provide more extensive location information than the J-Standard itself specifies.

however, that providing location information is consistent with those statutory criteria. For reasons that the Commission itself has recognized, location information is "call-identifying information," and therefore must be provided to law enforcement in order to "meet the assistance capability requirements" of Section 103. 47 U.S.C. § 1006(b)(1). Such information can be provided "by cost-effective methods" (*ibid.*), particularly in light of the fact that the same kind of information is already generated and used by wireless carriers for other purposes. As explained above, the J-Standard makes location information available only when law enforcement is judicially authorized to obtain it, and hence the J-Standard does not jeopardize "the privacy and security of communications not authorized to be intercepted." *Id.* § 1006(b)(2). The J-Standard's location information provisions should not materially affect residential ratepayers, nor should they interfere with "the provision of new technologies and services to the public." *Id.* § 1006(b)(3)-(4). Finally, we agree with the Commission (see Notice ¶¶ 46, 55) that the compliance deadline of June 30, 2000, previously established by the Commission should be sufficient for development and implementation of this feature.

B. Separation of Call Content and Call-Identifying Information in Packet Mode Communications

CDT's petition presents a discrete objection to the J-Standard's treatment of packet mode communications. The J-Standard requires carriers transmitting communications using packet switching protocols to deliver the entire packet data stream associated with a given communication, including call content, except where information is not authorized to be acquired. See J-STD-025 § 4.5.2, ¶ 2 (Packet Data IAP). CDT has asserted that this aspect of the J-Standard violates Section 103(a)(4)(A) of CALEA, which requires carriers to "protect[] * * * the privacy and security of

communications and call-identifying information not authorized to be intercepted * * * ." 47 U.S.C. § 1002(a)(4)(A). CDT has asked the Commission to modify the J-Standard to require carriers to strip out call content from the packet data stream when law enforcement is operating on the basis of pen register authority, so that call content that law enforcement is not authorized to intercept is not transmitted. See Notice ¶ 59; CC Docket No. 97-213, CDT Comments at 34-38 (filed May 20, 1998).

The Commission has not reached a tentative conclusion regarding CDT's proposal. Instead, it has requested additional comments and information. The Commission is seeking comments not only on the specific packet mode issue raised by CDT, but also on more general issues regarding how CALEA should be applied to packet mode communications. See Notice ¶¶ 63-66. In response to the Commission's request, we first address the specific issue raised by CDT: whether Section 103(a)(4)(A) requires carriers to remove call content from packets that are sent to law enforcement on the basis of pen register authority. We then address the broader packet mode issues identified in the Notice.

1. At the outset, we wish to make one point very clear: the government has no desire to receive call content from carriers when its legal authority does not entitle it to intercept call content. As a result, if the J-Standard had provided for carriers to strip out call content from the packet stream in pen register cases, as CDT proposes, rather than relying on law enforcement to perform that function, the government would have been -- and still would be -- satisfied with such an arrangement. The initiative for delivering "full" packets to law enforcement, even in pen register cases, has come from industry, not from law enforcement.

Having said that, however, we must be equally clear in saying that the J-Standard's treatment of packet mode communications in pen register cases does not conflict with anything in CALEA, and hence the J-Standard is not legally deficient in this regard. See Government May Comments at 21-22. As we have explained previously, CALEA amended the pen register statute (18 U.S.C. §§ 3121 et seq.) to require law enforcement to "use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing and signaling information utilized in call processing." 18 U.S.C. 3121(c) (added by Section 207(b)(2) of CALEA). As a technical matter, it is perfectly feasible for law enforcement to employ equipment that distinguishes between a packet's header and its communications payload and makes only the relevant header information available for "recording or decoding."¹⁰ In pen register cases involving packet mode communications, the J-Standard simply -- and quite permissibly -- relies on law enforcement to comply with its legal obligations under 18 U.S.C. § 3121(c) in this fashion.

The Notice suggests that if a carrier were to deliver both call-identifying information and call content to law enforcement in a pen register case, it would "seem" (Notice ¶ 63) to violate the carrier's obligation under Section 103(a)(4)(A) to "protect[] * * * the privacy and security of communications and call-identifying information not authorized to be intercepted * * * ." But that is what has always happened in pen register cases in the analog environment. As we have explained before, and as CDT itself has acknowledged, when garden-variety pen register surveillance is carried out over the "local loop" between the subscriber and the central office, law enforcement receives

¹⁰ The ability to distinguish between headers and payload is inherent in packet mode protocols. The position of the payload within the packet either is identified in the header or is defined (*i.e.*, fixed) by the protocol itself. With that information in hand, it is technically trivial to strip out the payload.

access to all signals transmitted over the subscriber's line on the local loop, including call content as well as dialing and signaling information. In such cases, the signals are sent to a device that is configured to record and decode the dialing and signaling information utilized in call processing (see p. 26 supra) without recording or disclosing the call content. Nothing in the language or legislative history of CALEA indicates that Congress meant to prohibit this longstanding arrangement. It is worth noting that Section 103(a)(4) does not state that carriers "shall not deliver" communications and call-identifying information that law enforcement is not authorized to intercept, but only that carriers shall "protect the privacy and security" of such information. A carrier is entitled to rely on law enforcement's discharge of its legal obligation under 18 U.S.C. § 3121(c) as a means of "protecting the privacy and security" of information that law enforcement is not authorized to intercept. Accordingly, the J-Standard is not deficient in this regard.

2. In connection with CDT's specific challenge to the J-Standard's packet mode provisions, the Commission has posed a number of broader questions about the application of CALEA to packet mode communications. See Notice ¶ 65. The Commission has asked for comments on "whether and, if so, how the statutory requirements of Section 103(a) of CALEA apply to packet-mode communications." Ibid. The Commission asks for comments on what constitutes "the equivalent of 'call-identifying information' for packet-mode telecommunications services within the context of CALEA." Ibid. And the Commission asks whether packet-mode call-identifying information "[w]ill * * * be 'reasonably available' to carriers and, thus, subject to the provisions of Section 103(a)(2) of CALEA." Ibid.

We understand the Commission's interest in developing a fuller understanding of how CALEA applies to packet mode communications. However, we urge the Commission to proceed

cautiously and not to take on unnecessary burdens in this regard. CDT's specific challenge to the J-Standard can be resolved without the need to resolve broader questions that may arise concerning the relationship between CALEA and packet mode communications. And if the Commission agrees that the J-Standard is not deficient in the specific respect identified by CDT, there is no need -- and no basis -- for the Commission to go further. As the Commission itself has stated, "the uncontested technical requirements [of the J-Standard] are beyond the scope of this proceeding." Notice ¶ 45 (emphasis added). CDT's rulemaking petition contests only one provision of the J-Standard involving packet mode communications (J-STD-025 § 4.5.2). As a result, other provisions of the J-Standard that may relate to packet mode communications are simply not within the scope of this proceeding, and absent any claim (much less any determination) that they are deficient, they are not subject to the Commission's standard-setting authority under Section 107(b).

Having said that, we offer the following comments on the general questions that the Commission has raised concerning packet mode communications. First, CALEA's assistance capability requirements do not draw any distinction between packet mode communications and circuit mode communications.¹¹ The obligations imposed by Section 103 apply equally to all "telecommunications carriers," meaning all "person[s] or entit[ies] engaged in the transmission or switching of wire or electronic communications as a common carrier for hire * * * ." 47 U.S.C. § 1001(8). The assistance capability requirements of Section 103 encompass all "wire and electronic communications," and all associated call-identifying information, carried by such carriers. *Id.* § 103(a)(1)-(2). If a telecommunications carrier is transmitting a "wire communication" or an

¹¹ For a general discussion of the difference between packet mode communications and circuit mode communications, see J-STD-025, Annex B, § B.1.

"electronic communication," as those terms are defined (18 U.S.C. § 2510(1), (12)), the carrier must comply with Section 103 with respect to those communications, regardless of whether the carrier is using packet-mode technology or some other technology to transit the communications. Thus, to answer the Commission's threshold question, the statutory requirements of Section 103 do apply to packet mode communications, just as they apply to communications that are not transmitted using packet mode protocols.

As noted above in connection with our discussion of subject-initiated dialing and signaling information, CALEA does draw a statutory distinction between "telecommunications carriers" and providers of "information services." See 47 U.S.C. §§ 1001(6), 1001(8)(C)(i), 1002(b)(2)(A). This statutory distinction, however, does not correspond to any distinction between packet mode communications and circuit mode communications. A telecommunications carrier can use either packet mode or circuit mode technology to transmit wire and electronic communications. The use of packet mode protocols does not turn the transmission of a wire or electronic communication by a telecommunications carrier into the provision of information services.

As for what constitutes "the equivalent of 'call-identifying information' for packet-mode telecommunications services within the context of CALEA" (Notice ¶ 65), the starting point for analysis is the statutory definition of "call-identifying information" itself. "Call-identifying information" encompasses all "dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier." 47 U.S.C. § 1001(2). When information is transmitted using packet mode protocols, "call-identifying information" therefore would encompass all information that identifies (or is required to identify) the "origin, direction,

destination, or termination" of the communication packet -- in short, all information used in routing the packet.

This information will be included in the parameters found in the packet header. In the case of connectionless packet mode services (Notice ¶ 65), the header of each packet will identify the packet's origin and destination addresses. In the case of connection-oriented packet mode services (ibid.), the packet header contains a connection identifier that is associated with the origin and destination addresses. The specific parameters that identify the "origin, direction, destination, or termination" of the packet will vary depending on the data service and protocols involved.

Finally, whether packet-mode call-identifying information "[w]ill * * * be 'reasonably available' to carriers" (Notice ¶ 65) cannot be answered categorically, any more than one can state categorically whether circuit-mode call-identifying information will be reasonably available to carriers. The general definition of "reasonably available" that we have proposed above (see p. 25 supra) should be equally applicable to packet mode communication and circuit mode communications. Whether particular call-identifying information is reasonably available under this definition may vary among carriers, hardware platforms, and packet protocols. As long as a packet stream can be accessed, it is technically straightforward to isolate the parameters in the packet header that constitute call-identifying information, as indicated above.

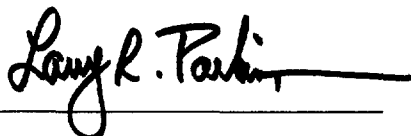
DATE: December 14, 1998

Respectfully submitted,


Louis J. Freeh, Director
Federal Bureau of Investigation

Honorable Janet Reno
Attorney General of the United States

Donald Remy
Deputy Assistant Attorney General

A handwritten signature in cursive script, reading "Larry R. Parkinson", written over a horizontal line.

Larry R. Parkinson
General Counsel
Federal Bureau of Investigation
935 Pennsylvania Avenue, N.W.
Washington, D.C. 20535

A handwritten signature in cursive script, reading "Douglas N. Letter", written over a horizontal line.

Douglas N. Letter
Appellate Litigation Counsel
Civil Division
U.S. Department of Justice
601 D Street, N.W., Room 9106
Washington, D.C. 20530
(202) 514-3602

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In the Matter of:)

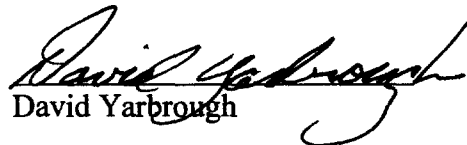
Communications Assistance for Law)
Enforcement Act)
_____)

CC Docket No. 97-213

Certificate of Service

I, David Yarbrough, a Supervisory Special Agent in the office of the Federal Bureau of Investigation (FBI), Washington, D.C., hereby certify that, on December 14, 1998, I caused to be served, by first-class mail, postage prepaid (or by hand where noted) copies of the above-referenced Comments Regarding Further Notice of Proposed Rulemaking, the original of which is filed herewith and upon the parties identified on the attached service list.

DATED at Washington, D.C. this 14th day of December, 1998.


David Yarbrough

**IN THE MATTER OF:
COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT
CC DOCKET 97-213
SERVICE LIST**

*The Honorable William E. Kennard
Chairman
Federal Communications Commission
1919 M Street N.W., Room 814
Washington, D.C. 20554

*The Honorable Harold Furchtgott-Roth
Commissioner
Federal Communications Commission
1919 M Street N.W., Room 802
Washington, D.C. 20554

*The Honorable Susan Ness
Commissioner
Federal Communications Commission
1919 M Street N.W., Room 832
Washington, D.C. 20554

*The Honorable Michael Powell
Commissioner
Federal Communications Commission
1919 M Street, N.W., Room 844
Washington, D.C. 20554

*The Honorable Gloria Tristani
Commissioner
Federal Communications Commission
1919 M Street, N.W., Room 826
Washington, D.C. 20554

*Ari Fitzgerald
Legal Advisor to Chairman Kennard
Federal Communications Commission
1919 M Street, N.W., Room 814
Washington, D.C. 20554

*James Casserly

Legal Advisor to Commissioner Ness
Federal Communications Commission
1919 M Street, N.W., Room 832
Washington, D.C. 20554

*Paul E. Misener

Senior Legal Advisor to Commissioner Furchtgott-Roth
Federal Communications Commission
1919 M Street, N.W., Room 802
Washington, D.C. 20554

*Peter A. Tenhula

Legal Advisor to Commissioner Powell
Federal Communications Commission
1919 M Street, N.W., Room 844
Washington, D.C. 20554

*Karen Gulick

Legal Advisor to Commissioner Tristani
Federal Communications Commission
1919 M Street, N.W., Room 826
Washington, D.C. 20554

*Christopher J. Wright

General Counsel
Federal Communications Commission
445 12th Street, S.W., Room 8C755
Washington, D.C. 20554

*Lawrence E. Strickling

Chief
Common Carrier Bureau
Federal Communications Commission
1919 M Street N.W., Room 500
Washington, D.C. 20554

*Gerald Vaughan

Acting Chief
Wireless Telecommunications Bureau
Federal Communications Commission
2025 M Street, N.W., Room 5002
Washington, D.C. 20554

***Thomas Sugrue**
Chief
Wireless Telecommunications Bureau
Federal Communications Commission
2025 M Street, N.W., Room 5002
Washington, D.C. 20554

***David Wye**
Technical Advisor
Federal Communications Commission
2025 M Street, N.W., Room 5002
Washington, D.C. 20554

***Anna Gomez**
Chief
Network Services Division
Common Carrier Bureau
Federal Communications Commission
2000 M Street N.W., Room 235B
Washington, D.C. 20554

***Kent Nilsson**
Office of Engineering and Technology
Federal Communications Commission
2000 M Street N.W.
Washington, D.C. 20554

***Charles Iseman**
Office of Engineering and Technology
Federal Communications Commission
2000 M Street, N.W., Room 424
Washington, D.C. 20554

***Jim Burtle**
Office of Engineering and Technology
Federal Communications Commission
2000 M Street, N.W., Room 281
Washington, D.C. 20554

*Julius Knapp
Office of Engineering and Technology
Federal Communications Commission
2000 M Street, N.W., Room 425
Washington, D.C. 20554

*Rodney Small
Office of Engineering and Technology
Federal Communications Commission
2000 M Street, N.W., Room 480
Washington, D.C. 20554

*Geraldine Matise
Office of Engineering and Technology
Federal Communications Commission
2000 M Street, N.W., Room 480
Washington, D.C. 20554

*Charlene Lagerwerff
Wireless Telecommunications Bureau
Federal Communications Commission
2100 M Street, N.W., Room 8633
Washington, D.C. 20554

*James Green
Wireless Telecommunications Bureau
Federal Communications Commission
2100 M Street, N.W., Room 7021
Washington, D.C. 20554

*Tejal Mehta
Wireless Telecommunications Bureau
Federal Communications Commission
2100 M Street, N.W., Room 7115
Washington, D.C. 20554

*David O. Ward
Network Services Division
Common Carrier Bureau
Federal Communications Commission
2000 M Street, N.W., Room 210
Washington, D.C. 20554

Matthew J. Flanigan
President
Telecommunications Industry Association
Suite 300
2500 Wilson Boulevard
Arlington, VA 22201-3834

Stewart A. Baker
Tom Barba
Steptoe & Johnson LLP
1330 Connecticut Avenue, N.W.
Washington, D.C. 20036-1795

Thomas Wheeler
President & CEO
Cellular Telecommunications Industry Association
Suite 200
1250 Connecticut Avenue, N.W.
Washington, D.C. 20036

Albert Gidari
Perkins Coie
1201 Third Avenue
40th Floor
Seattle, Washington 98101

Mark J. Golden
Senior Vice President, Industry Affairs
Robert Hoggarth
Senior Vice President, Paging/Messaging
Personal Communications Industry Association
Suite 700
500 Montgomery Street
Alexandria, VA 22314-1561

Roy Neel
President & CEO
United States Telephone Association
Suite 600
1401 H Street, N.W.
Washington, D.C. 20005-2164

Alliance for Telecommunication Industry Solutions
Suite 500
1200 G Street, N.W.
Washington, D.C. 20005

Jerry Berman
Executive Director
Center for Democracy and Technology
Suite 1100
1634 Eye Street, N.W.
Washington, D.C. 20006

Mark C. Rosenblum
Ava B. Kleinman
Seth S. Gross
Room 3252F3
295 North Maple Avenue
Basking Ridge, NJ 07920

William L. Roughton, Jr.
Associate General Counsel
PrimeCo Personal Communications, L.P.
Suite 320 South
601 13th Street, N.W.
Washington, D.C. 20005

Pamela J. Riley
David A. Gross
AirTouch Communications, Inc.
1818 N Street, N.W.
Washington, D.C. 20036

Joseph R. Assenzo
4900 Main Street, 12th Floor
Kansas City, MO 64112

James P. Lucier, Jr.
Director of Economic Research
Americans for Tax Reform
Suite 200
1320 18th Street, N.W.
Washington, D.C. 20036

Lisa S. Dean
Director, Center for Technology Policy
Free Congress Foundation
717 Second Street, N.E.
Washington, D.C. 20002

Anita Sheth
Director, Regulatory Policy Studies
Citizens for a Sound Economy
Suite 700
1250 H Street, N.W.
Washington, D.C. 20005

James X. Dempsey
Senior Staff Counsel
Daniel J. Weitzner
Deputy Director
Center for Democracy and Technology
Suite 1100
1634 Eye Street, N.W.
Washington, D.C. 20006

Eric W. DeSilva
Stephen J. Rosen
Wiley, Rein & Fielding
1776 K Street, N.W.
Washington, D.C. 20006

Lawrence E. Sarjeant
Linda Kent
Keith Townsend
Suite 600
1401 H Street, N.W.
Washington, D.C. 20005

Michael Altschul
Vice President and General Counsel
Randall S. Coleman
Vice President, Regulatory Policy and Law
Cellular Telecommunications Industry Association
Suite 200
1250 Connecticut Avenue, N.W.
Washington, D.C. 20036

John Pignataro
Senior Technical Advisor
Police Department, City of New York
Fort Totten Building 610
Bayside, NY 11359

Barbara J. Kern
Counsel
Ameritech Corporation
4H74
2000 Ameritech Center Drive
Hoffman Estates, IL 60196

James D. Ellis
Robert M. Lynch
Durward D. Dupre
Lucille M. Mates
Frank C. Magill
175 E. Houston, Room 4-H-40
San Antonio, TX 78205

Robert Vitanza
Suite 1300
15660 Dallas Parkway
Dallas, TX 75248

M. Robert Sutherland
Theodore R. Kingsley
BellSouth Corporation
Suite 1700
1155 Peachtree Street, N.E.
Atlanta, GA 30309-3610

Michael P. Goggin
BellSouth Cellular Corp.
Suite 910
1100 Peachtree Street, N.E.
Atlanta, GA 30309-4599

Michael W. White
BellSouth Wireless Data, L.P.
10 Woodbridge Center Drive, 4th Floor
Woodbridge, NJ 07095-1106

J. Lloyd Nault, II
BellSouth Telecommunications, Inc.
4300 BellSouth Center
675 West Peachtree Street, N.E.
Atlanta, GA 30375

Charles M. Nalborne
Suite 400
3353 Peachtree Road, N.E.
Atlanta, GA 30326

Kurt A. Wimmer
Gerard J. Waldron
Alane C. Weixel
Ellen P. Goodman
Erin Egan
Covington & Burling
1201 Pennsylvania Avenue, N.W.
P.O. Box 7566
Washington, D.C. 20044-7566

William T. Lake
John H. Harwood II
Samir Jain
Todd Zubler
Wilmer, Cutler & Pickering
2445 M Street, N.W.
Washington, D.C. 20037-1420

Kathryn Marie Krause
Edward M. Chavez
1020 19th Street, N.W.
Washington, D.C. 20036

Martin L. Stern
Lisa A. Leventhal
Preston Gates Ellis & Rouvelas Meeds LLP
Suite 500
1735 New York Avenue, N.W.
Washington, D.C. 20006

*International Transcription Service, Inc.
1231 20th Street, N.W.
Washington, D.C. 20036

* Hand Delivered